

Download session keys with packet captures

Published: 2024-11-02

You can download PCAP Next Generation (pcapng) file that includes all captured TLS session keys and encrypted packets. You can then open the packet capture file in a tool such as Wireshark, which can apply the session keys and display the decrypted packets.

Before you begin

- You must have a configured packetstore or packet capture disk before you can download packets and session keys from a sensor or a console. See our [deployment guides](#) to get started.
- The console must be licensed for TLS Shared Secrets.
- The [TLS Session Key Storage](#) setting must be enabled on the sensor.
- RevealX Enterprise users must have either system access and administration [privileges](#) or limited privileges with packets and session keys access. RevealX 360 users must have packets and session keys access.

- Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
- From the top menu, click **Packets**.
- Optional: Apply filters to refine the packet query.
- When the query completes, click **Download PCAP + Session Keys**.
- Click **Download PCAP + Session Keys**.
The pcapng file is automatically downloaded to your computer and the session key download operation is recorded in the [audit log](#).

If there are no session keys available for the downloaded packet capture, the **Download PCAP + Session Keys** button does not appear.

View the decrypted payload in Wireshark

- Start the Wireshark application.
- Open the downloaded packet capture (pcapng) file in Wireshark.

When an SSL-encrypted frame is selected, the **Decrypted SSL** tab appears at the bottom of the Wireshark window. Click the tab to see the decrypted information in the packet capture as plain text.

The screenshot shows the Wireshark interface with a packet capture file named 'extrahop 2022-11-22 17.27.33 to 17.32.33 PST.pcapng'. The packet list pane shows several packets, with packet 340 selected. The packet details pane shows the following information:

No.	Time	Source	Destination	Protocol	Length	Info
331	125.5824110...	10.10.9.229	10.10.254.58	TCP	74	59934 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1162276 TSecr=227215419
333	125.5825180...	10.10.254.58	10.10.9.229	TCP	74	443 → 59934 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM TSval=1162276 TSecr=227215419
334	125.5825370...	10.10.9.229	10.10.254.58	TCP	66	59934 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1162276 TSecr=227215419
335	125.5825930...	10.10.9.229	10.10.254.58	TLSv1.2	583	Client Hello
336	125.5844130...	10.10.254.58	10.10.9.229	TLSv1.2	3041	Server Hello, Certificate, Server Key Exchange, Server Hello Done
337	125.5844440...	10.10.9.229	10.10.254.58	TCP	66	59934 → 443 [ACK] Seq=518 Ack=2976 Win=35200 Len=0 TSval=1162276 TSecr=227215419
338	125.5856400...	10.10.9.229	10.10.254.58	TLSv1.2	248	Client Key Exchange, Change Cipher Spec, Finished
339	125.5868430...	10.10.254.58	10.10.9.229	TLSv1.2	173	Change Cipher Spec, Finished
340	125.5869730...	10.10.9.229	10.10.254.58	HTTP	247	GET /. HTTP/1.0
341	125.5877090...	10.10.254.58	10.10.9.229	HTTP	1591	HTTP/1.1 401 Unauthorized (text/html)
342	125.5878320...	10.10.9.229	10.10.254.58	TLSv1.2	151	Alert (Level: Warning, Description: Close Notify)

The packet details pane for the selected packet (340) shows the following information:

- Frame 340: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface
- Ethernet II, Src: VMware_94:40:10 (00:50:56:94:40:10), Dst: VMware_94:4f:bc (00:50:56:94:4f:bc)
- Internet Protocol Version 4, Src: 10.10.9.229, Dst: 10.10.254.58
- Transmission Control Protocol, Src Port: 59934, Dst Port: 443, Seq: 700, Ack: 306
- Transport Layer Security
 - TLSv1.2 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 176
 - Encrypted Application Data: 37bc8ea8c8a18c9e67eaf5682ebc6ecbfbae2c95ad3de5c...
 - Hypertext Transfer Protocol